UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS

Jimmy Tuan Tran Plaintiff, vs. Defendant "1" a/k/a "Miko" and John Doe Defendants 1-4 who are the cohorts of Defendant "1" and are the owners of the following cryptocurrency deposit wallets where Plaintiff's stolen cryptocurrency assets were transferred: Binance: 0x7b338050e5002de4b4963401d73fb4ec507cc812 OKX: 0x71fbc4ba1608bb110ba9ee7725b6869cbf33a2bb HTX: 0x8552681ca9fdb2be3b383c4fd0e90b3789609253 and Crypto.com: 0x8c8cf418be7dce2f288486ccc7b3680293376c5f Defendant(s).	Civil Action No. _____

PLAINTIFF JIMMY TUAN TRAN'S COMPLAINT FOR VIOLATION OF THE RACKETEER INFLUENCED AND CORRUPT ORGANIZATIONS ACT

Plaintiff, Jimmy Tuan Tran ("Plaintiff"), by and through undersigned counsel, sues Defendant "1" a/k/a "Miko" and John Doe Defendants 1-4 ("Defendants"), as follows:

PRELIMINARY STATEMENT

1. Defendants stole 5,136 Tether (USDT), 140.05 Ethereum (ETH), and 172,043 USD Coin (USDC) from Plaintiff pursuant to a sophisticated global internet cryptocurrency fraud and conversion scheme, the current market value of which is six hundred sixty-two thousand eight

hundred fifty-five dollars and sixty cents ($662,855.60)[1].

2. Defendant "1" played a material role in the theft of Plaintiff's assets, and upon information and belief, she and her cohorts currently possess all or a significant portion of Plaintiff's stolen property.

3. Plaintiff brings this lawsuit to recover his stolen assets.

SUBJECT MATTER JURISDICTION AND VENUE

4. This is an action for damages related to the theft of Plaintiff's cryptocurrency assets as detailed below. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332 (diversity jurisdiction). This action includes damages pursuant to 18 U.S.C. § 1964 (the "Racketeer Influenced and Corrupt Organizations Act" or "RICO"). This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 (federal question).

5. Venue is proper in this District pursuant to 18 U.S.C. § 1965(a) and (b), and 28 U.S.C. § 1391(b) and (c).

6. Defendants are subject to personal jurisdiction in this district, because they direct business activities toward and conduct business with consumers throughout the United States, including within the State of Texas and this district through at least a fraudulent website (cme-crypto.org) which can be accessed on the internet and on smartphones and is accessible from Texas.

7. Plaintiff accessed the fraudulent website (cme-crypto.org) in the State of Texas and the theft occurred while Plaintiff was located in the State of Texas. Defendants directed numerous false and fraudulent representations to Plaintiff in this district, stole Plaintiff's assets within this district, and caused significant harm to Plaintiff in this district.

[1] Current market value calculated using data from etherscan.io on November 25, 2024.

8. Moreover, Defendants are foreign nationals and are subject to personal jurisdiction in this district pursuant to Federal Rule of Civil Procedure 4(k)(2) because (i) Defendants are not subject to jurisdiction in any state's court of general jurisdiction; and (ii) exercising jurisdiction is consistent with the United States Constitution and laws.

THE PARTIES AND PERSONAL JURISDICTION

9. Plaintiff, Jimmy Tuan Tran, an individual, is *sui juris*, and is a resident and citizen of Texas.

10. Defendant "1" is an individual, is sui juris, and is subject to the personal jurisdiction of this Court. Defendant "1" represented to Plaintiff Jimmy Tuan Tran that her name was "Miko". Defendant represented to Plaintiff that she was originally from Germany but currently living in Los Angeles, California.

11. John Doe Defendants 1-4 are the cohorts of Defendant "1" and are the owners of the following cryptocurrency deposit wallets where Plaintiff's stolen cryptocurrency assets were transferred:

- Binance:
  - 0x7b338050e5002de4b4963401d73fb4ec507cc812
- OKX:
  - 0x71fbc4ba1608bb110ba9ee7725b6869cbf33a2bb
- HTX:
  - 0x8552681ca9fdb2be3b383c4fd0e90b3789609253
- Crypto.com:
  - 0x8c8cf418be7dce2f288486ccc7b3680293376c5f

12. John Doe Defendants 1-4 are *sui juris* and subject to the personal jurisdiction of this court. John Doe Defendants 1-4 have intentionally concealed their identity as part of their scheme to defraud Plaintiff, but as part of their conspiracy directed fraudulent communications towards Plaintiff in Texas, causing Plaintiff to suffer significant economic and emotional harm

while in Texas.

13. At all times material hereto, Defendants have maintained and continue to maintain private cryptocurrency wallets and cryptocurrency exchange accounts in which all of or a portion of Plaintiff's stolen cryptocurrency currently sits.

ALLEGATIONS COMMON TO ALL COUNTS

A. Defendants Execute an International Cryptocurrency Theft Scheme

14. Plaintiff is a victim of not only a nationwide but also a worldwide RICO conspiracy known as "pig butchering."

15. Pig butchering scams are "fraudulent crypto investment schemes directed from Asia," which are now a billion-dollar industry.[2]

16. Pig butchering scams run and perpetrated by organized criminal groups in Southeast Asia, are called such because the victims are "likened to hogs fattened up for slaughter."[3]

17. The scammers, typically located in Southeast Asia, carefully research their victims, and can spend months grooming the victim to gain their trust.

18. Pig butchering scammers utilize expertly crafted copycat websites that replicate authentic trading platforms. These scammers simulate trades and returns and the victims are unaware of the scheme.[4]

19. The perpetrators of these so-called pig butchering scams befriend victims and over time build up trust. Once that trust is gained, the perpetrators claim to be experts in cryptocurrency investments, fraudulently represent themselves to be experts in cryptocurrency investing, and convince victims to send their digital assets to fake copycat exchanges.

[2] https://www.reuters.com/investigates/special-report/fintech-crypto-fraud-thailand/
[3] https://www.nbcnews.com/news/crime-courts/pig-butchering-scams-rise-fbi-moves-stop-bleeding-rcna137009
[4] https://www.reuters.com/investigates/special-report/fintech-crypto-fraud-thailand/

20. In September of 2023, FinCEN issued an alert to warn United States citizens of the threat of pig butchering scam, explaining:

> "Pig butchering" scams resemble the practice of fattening a hog before slaughter. Victims invest in supposedly legitimate virtual currency investment opportunities before they are conned out of their money. Scammers refer to victims as "pigs," and may leverage fictitious identities, the guise of potential relationships, and elaborate storylines to "fatten up" the victim into believing they are in trusted partnerships before they defraud the victims of their assets—the "butchering." These scams are largely perpetrated by criminal enterprises based in Southeast Asia who use victims of labor trafficking to conduct outreach to millions of unsuspecting individuals around the world.[5]

21. Likewise, in an alert warning United States citizens about these scams, the Office of the Inspector General explained, "[Pig butchering] is a type of confidence and investment fraud in which the victim is gradually lured into making increasing monetary contributions, generally in the form of cryptocurrency, to a seemingly sound investment before the scammer disappears with the contributed monies."[6]

22. Plaintiff had no experience trading cryptocurrency prior to being approached by Defendant "1" a/k/a "Miko".

23. Around June 2023, Plaintiff received a message on X (formerly known as "Twitter") from Defendant "1" a/k/a "Miko" who proceeded to conversate with Plaintiff and eventually requested to continue their communication through WhatsApp.

24. Within a few days of meeting, Defendant "1" misrepresented that she would help Plaintiff make an extra income by teaching Plaintiff how to become a successful cryptocurrency trader.

25. Defendant "1" lured Plaintiff by showing him examples over WhatsApp of how she was successfully earning high returns on her cryptocurrency trading methods.

---

[5] Exh. A, FinCEN Alert on Prevalent Virtual Currency Investment Scam Commonly Known as "Pig Butchering."
[6] Exh. B, Office of the Inspector General Warning on Pig Butchering Scams.

26. Defendant "1" represented to Plaintiff that she was using a trusted trading platform called cme-crypto.org.

27. Defendant "1" assisted Plaintiff in utilizing cme-crypto.org which she claimed was a legitimate decentralized trading exchange. She stated that "cme-crypto.org" would be used as a trading platform with the purpose of making transactions; and when done, the assets would be transferred to Plaintiff's wallet for withdrawal.

28. However, the application Defendant "1" provided to Plaintiff was not a legitimate exchange website owned and operated by any exchange but was instead a fraudulent website created to deceive individuals, including Plaintiff, into believing they were investing on a legitimate cryptocurrency exchange.

29. The fraudulent trading platform, cme-crypto.org, is no longer accessible.

30. To further entice Plaintiff into believing she was a legitimate investor who only wanted to assist Plaintiff in becoming a successful cryptocurrency trader like her, around June 2023, Defendant "1" had Plaintiff run a test where he transferred approximately one thousand dollars ($1000.00) worth of cryptocurrency from his Crypto.com and Kraken accounts into the fraudulent cme-crypto.org platform. When Plaintiff was able to transfer this amount back to his digital wallets, he believed that Defendant "1" was a legitimate investor who wanted to help him learn how to invest cryptocurrency and, further, that the fraudulent website he had accessed was also legitimate.

31. After familiarizing himself with the process of trading on the fraudulent website recommended by Defendant "1," and in reliance on the foregoing false and fraudulent misrepresentations, Plaintiff started to transfer cryptocurrency from his Crypto.com and Kraken accounts, legitimate third-party online platforms for buying, selling, transferring, and storing

cryptocurrency, to the fraudulent platform.

32. Defendants posted fraudulent returns on their fake website which made it appear that Plaintiff was making money on his trades.

33. As a result, he continued to transfer cryptocurrency from his Crypto.com and Kraken accounts to the fraudulent exchange. Because of the fraudulent representations contained on the fake cme-crypto.org platform, and misrepresentations made by Defendant "1", Plaintiff believed that he had made significant money from his previous investments.

34. Plaintiff was told by Defendant "1" that the value of his cryptocurrency had grown significantly, which was reflected on the fraudulent cme-crypto.org statements.

35. Plaintiff was happy with what he believed was a significant return on Plaintiff's investment. However, when Plaintiff decided it was time to transfer all the cryptocurrency from cme-crypto.org back to Plaintiff's Crypto.com and Kraken accounts, he discovered that his funds had been frozen.

36. Plaintiff attempted to reach what he thought was cme-crypto.org help desk to get an explanation on why his funds had been frozen. Eventually, Plaintiff received a response from "support@cme-crypto.org" stating that would have to pay twenty thousand three hundred dollars ($20,300.00) in bail to release his invested funds.

37. This is when Plaintiff realized he had been scammed. Plaintiff refused to pay the additional twenty thousand and three hundred dollars ($20,300.00) and made numerous unsuccessful attempts to transfer the cryptocurrency from the fake exchange back to his Crypto.com and Kraken wallets.

B. Plaintiff's Forensic Tracing of His Stolen Cryptocurrency

38. When a transaction is made on the blockchain it is assigned a "transaction hash"

("TXID"). A transaction hash is a unique string of characters that is given to every transaction that is verified and added to the blockchain. A TXID is used to uniquely identify a particular transaction. All on-chain transactions (the transactions from or to external addresses) have a unique TXID that can be seen in transaction details. All on-chain transactions (depositing and withdrawing of funds) have a unique TXID that can be found in transaction details.

39. Within the time frame of June 24, 2023, and November 1, 2023, Plaintiff made 23 transactions from his Crypto.com and Kraken accounts to the fraudulent exchange. In total, Plaintiff transferred approximately 5,136 Tether (USDT), 140.05 Ethereum (ETH), and 172,043 USD Coin (USDC) to the fraudulent exchange, which had a market value at the time of approximately four hundred thirty-four thousand and sixty-six dollars ($434,066.00).

40. Plaintiff has retained forensic cryptocurrency tracing experts who have traced Plaintiffs stolen assets on the blockchain. Attached hereto as Exhibit "A" is the tracing report completed by experts at CipherBlade, LLC. Plaintiff incorporates Exhibit "A" into his verified complaint.

41. As the tracing shows, Defendant "1" with the help of multiple co-conspirators opened numerous cryptocurrency wallets owned by John Doe Defendants 1-4 to launder the stolen cryptocurrency to the identified foreign cryptocurrency exchange.

COUNT I
RACKETERING IN VIOLATION OF 18 U.S.C. § 1964

42. The operation of Defendant "1" and John Doe Defendants 1-4, individually and through their alleged business in trading cryptocurrency as cryptocurrency traders in their sophisticated global internet cryptocurrency fraud and conversion scheme constitutes a racketeering operation.

43. Defendant "1" directed and coordinated with John Doe Defendants 1-4 as yet

unidentified additional parties ("RICO Enterprise," or "Enterprise") within the meaning of 18 U.S.C. § 1964(4), which Enterprise was engaged in, or the affairs of which affected, interstate and foreign commerce.

44. Defendant "1" and John Doe Defendants 1-4 were each also a member of the RICO Enterprise, as each was a distinct person, separate and apart, from each of the RICO Enterprise members together.

45. The RICO Enterprise engaged in a pattern of racketeering activity.

46. Each person's participation was effective partly because each mimicked an actual on-going business (including the fraudulent platform cme-crypto.org) with a presence in the marketplace: the United States and indeed worldwide.

47. As co-conspirators, the unlawful conduct of each member of the RICO Enterprise is attributed to every member, i.e. Defendant "1" and John Doe Defendants 1-4 as yet unidentified co-conspirators.

48. As set forth above, the RICO Enterprise engaged in the following predicate acts of racketeering within the meaning of 18 U.S.C. § 1961(1): Wire fraud in violation of 18 U.S.C. § 1343.

49. The predicate acts set forth in this Complaint, include defrauding Plaintiff beginning in June 2023, through domestic and international telephone communication including X (formerly known as "Twitter") and WhatsApp messaging.

50. The predicate acts set forth in this Complaint are related, in that they have the same or similar purposes, results, participants, and methods of commission, and are otherwise interrelated by distinguishing characteristics and are not isolated events. The related criminal schemes set forth in this Complaint constitutes a "pattern or patterns of racketeering activity" as

defined in 18 U.S.C. § 1961(5).

51. The Defendants engaged in two or more predicated acts of racketeering within a period of ten years and committed at least one such act after October 15, 1970.

52. The information that would establish further predicate acts and further acts of racketeering is solely within the control of Defendants. Plaintiff requires discovery to ferret out the further extent of predicate acts and further acts of racketeering, including the identity of similarly situated defrauded victims and the scope of the systematic fraud.

53. Defendants have received income derived, directly or indirectly, from a pattern of racketeering activity and used or invested, directly or indirectly, part of such income, or the proceeds of such income, in acquisition of an interest in, or in the establishment or operation of, the RICO Enterprise, an enterprise which is engaged in, or the activities of which affect, interstate or foreign commerce in violation of 18 U.S.C. § 1962(a).

54. Defendants through a pattern of racketeering activity maintain, directly or indirectly, an interest in or control of the RICO Enterprise, an enterprise which is engaged in, or the activities of which affect, interstate or foreign commerce in violation of 18 U.S.C. § 1962(b).

55. Defendant "1" was associated with the RICO Enterprise, and conducted or participated, directly or indirectly, in the conduct of the Enterprise's affairs through the pattern of racketeering activity described herein in violation of 18 U.S.C. § 1962(c).

56. Defendant "1" and/or John Doe Defendants 1-4 as yet unidentified additional parties, each entered into a conspiracy to conduct or participate, directly or indirectly, in the conduct of the RICO Enterprises' affairs through the pattern of racketeering activity described herein, in violation of 18 U.S.C. § 1962(d).

57. As a direct and proximate result of Defendants' unlawful actions, Plaintiff has

suffered damages.

WHEREFORE, Plaintiff Jimmy Tuan Tran demands that judgment be entered against Defendant "1" and John Doe Defendants 1-4, jointly and severally, as follows:

(a) damages;

(b) statutory trebled damages pursuant to 18 U.S.C. § 1964(c);

(c) punitive damages;

(d) costs, including reasonable attorney's fees, pursuant to 18 U.S.C. § 1964(c);

(e) costs;

(f) interest; and

(g) such other and further relief as this Court deems just and proper.

COUNT II
CONVERSION

58. Through fraudulent misrepresentations, Defendants convinced Plaintiff to invest his money into cryptocurrency.

59. Defendants then convinced Plaintiff to transfer his cryptocurrency to the fake exchange owned and operated by Defendants.

60. After Plaintiff transferred his cryptocurrency assets to the fake exchange, Defendants then transferred Plaintiff's cryptocurrency to cryptocurrency addresses owned by Defendant "1" and John Doe Defendants 1-4.

61. Defendants misappropriated Plaintiff's funds.

62. Defendants have converted Plaintiff's funds to their own use or to the use of others not entitled thereto and have exercised dominion and control over the funds to Plaintiff's exclusion

and detriment.

63. Plaintiff has suffered damages as a direct and proximate result of Defendants' conversion.

WHEREFORE, Plaintiff Jimmy Tuan Tran demands that judgment be entered against Defendant "1" and John Doe Defendants 1-4, jointly and severally, for damages, interest, costs, and such other and further relief as this Court deems just and proper.

COUNT III
UNJUST ENRICHMENT

64. Plaintiff conferred a direct benefit upon Defendants by transferring the valuable cryptocurrency that Defendants converted from Plaintiff.

65. Defendants have knowledge of the benefit Plaintiff conferred upon them and have retained such benefit.

66. The circumstances under which Plaintiff conferred, and Defendants accepted, render Defendants' retention of the benefits inequitable.

67. Equity required that Defendants return to Plaintiff the benefits he conferred upon Defendants.

WHEREFORE, Plaintiff Jimmy Tuan Tran demands that judgment be entered against Defendant "1" and John Doe Defendants 1-4, jointly and severally, for damages, interest, costs, and such other further relief as this Court deems just and proper.

COUNT IV
IMPOSITION OF CONSTRUCTIVE TRUST AND DISGORGEMENT OF FUNDS

68. This is an action to impose a constructive trust upon the property taken from Plaintiff that is currently held by Defendants.

69. This action further calls for the restoration to Plaintiff of that wrongfully obtained

property.

70. As set forth above, Defendants – through actual fraud, misappropriation, conversion, theft, or other questionable means – obtained Plaintiff's cryptocurrency, which in equity and good conscience Defendants should not be permitted to hold.

71. The cryptocurrency assets at issue are specific identifiable property and have been traced to Binance, OKX, HTX, and Crypto.com.

72. Any and all assets being held by Defendants at Binance, OKX, HTX, and Crypto.com must be held in trust for Plaintiff's benefit, and Defendants are not entitled to the benefit of wrongfully misappropriated, converted and stolen cryptocurrency assets that were taken from Plaintiff.

73. The digital assets identified herein which are being held by Defendants at Binance, OKX, HTX, and Crypto.com must be disgorged to Plaintiff's benefit, as Defendants are not entitled to the benefit of wrongfully misappropriated, converted, and stolen cryptocurrency assets that were taken from Plaintiff.

WHEREFORE, Plaintiff Jimmy Tuan Tran demands the equitable imposition of a constructive trust over the property taken from Plaintiff that is currently under the control of Defendant "1" and/or John Doe Defendants 1-4, in the identified cryptocurrency wallet addresses held at Binance, OKX, HTX, and Crypto.com and further demands that the wrongfully obtained property be returned to Plaintiff.

COUNT V
CONSPIRACY

74. The Defendants conspired and confederated with each other to commit, and committed, Conversion (Count II); and Unjust Enrichment (Count III).

75. Relying on the false statements made by Defendant "1", including that she was an

expert in cryptocurrency investments, Plaintiff transferred his cryptocurrency assets to fake cryptocurrency platforms which were in actuality deposit addresses owned by John Doe Defendants 1-4.

76. Defendants conspired with others via the fraudulent website cme-crypto.org, X (formerly known as "Twitter"), and WhatsApp where they communicated with Plaintiff. Defendant "1" and John Doe Defendants 1-4 are the owners of the cryptocurrency deposit addresses where Plaintiff's stolen cryptocurrency was transferred.

77. As a result, Plaintiff has suffered damages as a direct and proximate result of Defendants' conspiracy.

WHEREFORE, Plaintiff Jimmy Tuan Tran demands that judgment be entered against Defendant "1" and John Doe Defendants 1-4, jointly and severally, for damages, interest, costs, and such other and further relief as this Court deems just and proper.

DEMAND FOR A JURY TRIAL

Plaintiff demands trial by jury on all issues so triable.

VERIFICATION

I, JIMMY TUAN TRAN, hereby declare under penalty of perjury that I have read the foregoing COMPLAINT FOR CONVERSION OF STOLEN CRYPTOCURRENCY and verify under penalty of perjury that all statements [redacted] e best of my knowledge, understanding, and belief.

Dated: November 25, 2024

_____
J[redacted]

Dated: November 26, 2024

Respectfully Submitted,

/s/ Marshal J. Hoda
Marshal J. Hoda, Esq.
Tx. Bar No. 24110009
THE HODA LAW FIRM, PLLC
3120 Southwest Fwy
Ste. 101 PMB 51811
Houston, TX 77098
Telephone: 832-848-0036
marshal@thehodalawfirm.com

/s/ Reagan Charleston Thomas
Reagan Charleston Thomas, Esq.
Attorney-in-Charge
(Pending Pro Hac Vice)
La. Bar No. 38522
AYLSTOCK, WITKIN, KREIS & OVERHOLTZ, PLLC
17 East Main Street, Suite 200
Pensacola, FL 32502
Telephone: 850-202-1010
Fax: 850-916-7449
rthomas@awkolaw.com

Attorneys for Plaintiff